IstroSec

Data Sheet

# Reakcia na útoky typu BEC

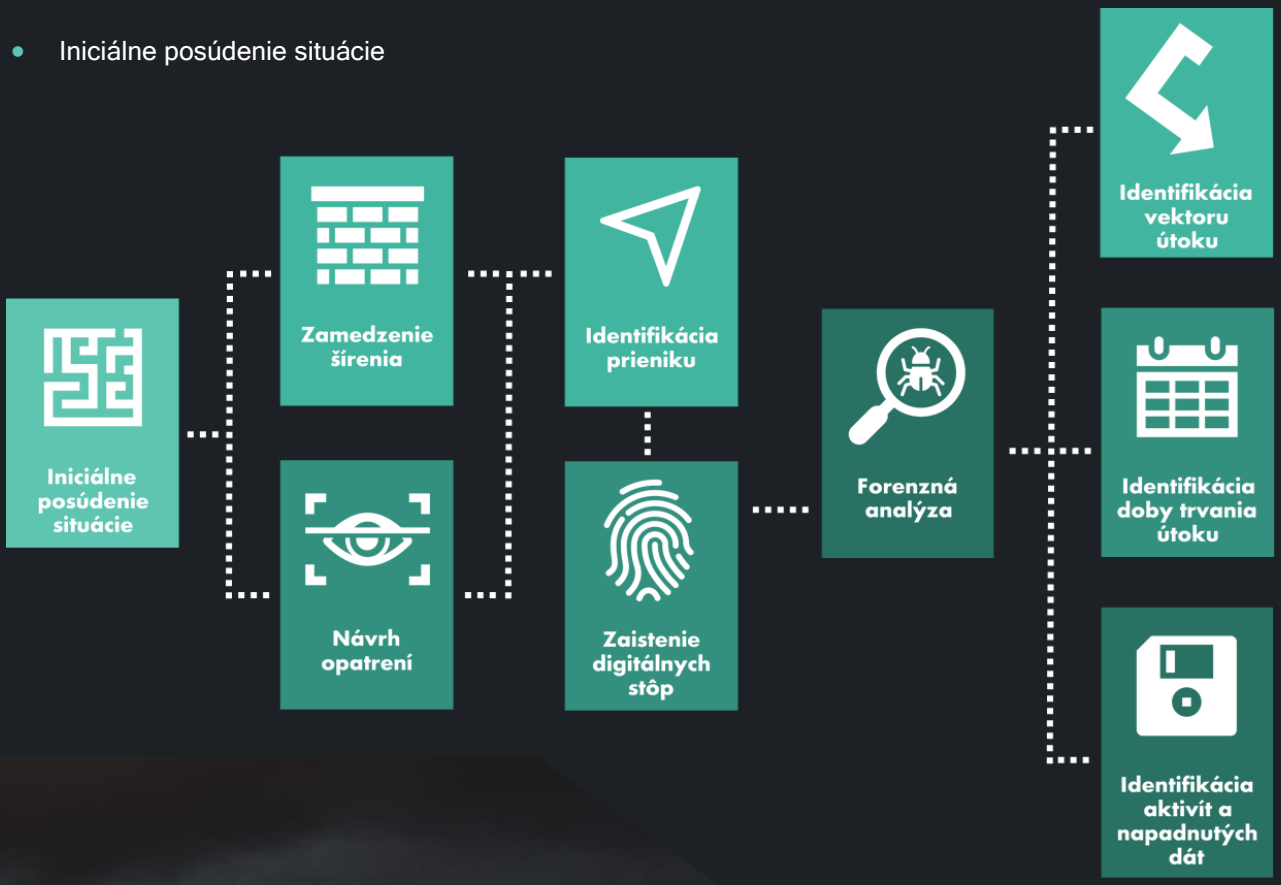
Business email compromise (BEC, kompromitácia emailového účtu) je typ útoku, ktorý sa sústreďuje na kompromitáciu jedného, alebo viacerých účtov a ich zneužitie na zaslanie podvodných emailov, alebo ďalšiu kompromitáciu organizácie. Podvodné emaily zasielané z kompromitovaných účtov sú používané na šírenie škodlivého kódu, posielanie falošných správ s cieľom získať finančný prospech alebo ďalšiu kompromitáciu.

## Aktivity v rámci služby

Útoky tohto typu sa vyskytujú na riešeniach vo vlastnej infraštruktúre ako aj u poskytovateľov cloudových služieb. V oboch prípadoch je v prípade nedostatočného zabezpečenia možné kompromitovať celý účet, prípadne celého nájomníka (cloud tenant). Prosím kontaktujte nás 24/7 na čísle: +421 917 699 002 alebo na email incident@istrosec.com.

Experti **Istro**Sec Vám pomôžu s vykonaním s reaktívnych aktivít na rýchle a efektívne vyriešenie tohto incidentu ku ktorým patrí:

- Iniciálne posúdenie situácie
- Zamedzenie šírenia kompromitácie
- Návrhom a implementáciou bezpečnostných opatrení na predchádzanie (zamedzenie pokračovania) tohto typu útokov
- Identifikácia prieniku, zaistenie digitálnych stôp a forenzná analýza prieniku
- Identifikácia vektoru útoku, časového okna útoku a aktivít vykonaných útočníkom v systéme
- Identifikácia dát, ku ktorým útočník pristupoval alebo ich sťahoval, prípadne modifikoval



IstroSec

Data Sheet

## Prečo práve my?

Špecialisti **Istro**Sec majú skúsenosti s reakciou na útoky typu BEC v rámci klientovej on-premise infraštruktúry aj v cloude (Office 365, Gmail, webmailové účty). Poznajú taktiky, techniky a postupy používané útočníkmi a majú znalosti potrebné na rýchlu, efektívnu a komplexnú reakciu.

### Efektívna reakcia

V prípade kybernetického útoku (najmä cieleného, alebo vykonávaného pokročilým útočníkom (tzv. APT) je potrebné reagovať v rádoch hodín, identifikovať momentálne prioritné úlohy a vykonať potrebné aktivity okamžite. Špecialisti **Istro**Sec majú skúsenosti s krízovým manažmentom v takýchto situáciách a podľa požiadaviek klienta koordinujú aktivity reakcie na incidenty alebo priamo tento proces riadia. **Istro**Sec má k dispozícii proprietárne nástroje, ktoré implementuje v rámci organizácie umožní tak efektívne izolovanie (containment) útoku a jeho analýzu.

### Prečo IstroSec?

Kombinované skúsenosti expertov viac ako 70 rokov

Prístup k odborníkom na všetky oblasti informačnej bezpečnosti, vrátane audítorov, penetračných testerov, forenzných analytikov, analytikov malvéru, školiteľov a ďalších

Systematické zlepšenie informačnej bezpečnosti v zmysle štandardov a na základe skúseností s riešením pokročilých bezpečnostných incidentov

Certifikovaní odborníci a zaistenie súladu s bezpečnostnými štandardmi a legislatívou - skúsenosti z verejnej správy (zákon o kybernetickej bezpečnosti, zákon o ITVS a iné) ako aj zo súkromného sektora (ISO 27001, NIST, HIPAA a iné)

### Podpora cieľovej organizácie

Špecialisti **Istro**Sec majú expertízu v oblasti reakcie na incidenty, forenznej analýzy a analýzy malvéru na svetovej úrovni, ktorú viackrát preukázali pri riešení štátmi sponzorovaných kybernetických útokov, útokov vedených voči organizáciám FORTUNE 500 ako aj účasťou 4 expertov spoločnosti **Istro**Sec vo víťaznom tíme cvičenia LockedShields 2016.

### Expertíza v riešení kybernetických útokov, v analýze malvéru a forenznej analýze

Experti **Istro**Sec sú držiteľmi medzinárodne uznávaných certifikátov v mnohých oblastiach. Držíme certifikáty, ako napríklad Certified Information Systems Security Professional (CISSP), Certified Information system Auditor (CISA), GIAC Certified Forensic Analyst (GCFA), GIAC Certified Forensic Examiner (GCFE), Certified Reverse Engineering Analyst (CREA) a ďalšie.